# SCIENCE & SECURITY March 2015

CASRA NEWSLETTER – ISSUE 9

A person with the intent to harm the aviation system most likely carries one or several items to execute the planned attack. Accordingly, threat items are an important focus in airport security controls. However, attackers are highly motivated to get through the controls without being detected. Therefore, threat items might be hard to discover, for example because they are well hidden or new and different to previously used items.

Behavioral Security Screening (BSS) offers an option for security controls that does not focus on threat items, but on behavioral cues to identify malicious intent. Despite an international interest in BSS, the debate on how such programs are best designed and implemented is ongoing. CASRA performed a scoping study to investigate these issues and the necessary steps to implement BSS as a security measure. The results are summarized in a comprehensive six-step implementation process that is presented in the section "Research Put Across".

A different approach to deal with the fact that attackers will always try to outwit the security system is to keep track of new and emerging threats and attack plans. This is what is done in CASRA's Systematic Threat Assessment (STA), which is an in-depth analysis of information on terrorist activities with the goal to make the results available for relevant stakeholders and to create countermeasures such as training programs for airport security screeners. You find the interesting article on the STA in the section "Security in Practice".

We hope that spring soon sends you its first welcome signs and wish you all the best,

Prof. Dr. Adrian Schwaninger

Dr. Diana Hardmeier

**TOPICS IN THIS ISSUE:**

RESEARCH PUT ACROSS

### APPROACHING SECURITY FROM ANOTHER ANGLE - BEHAVIORAL SECURITY SCREENING

Security screening processes at airports are still mainly focused on finding prohibited items. However, a growing number of authorities worldwide are interested in security measures at airports that also focus their attention on malicious intent: Trained personnel are scanning travelers for suspicious behavioral cues to identify wrongdoers. However, the question what form such a behavioral security screening (BSS) program should take or how it should be implemented is still in an investigation phase. CASRA conducted an 18-months scoping study, leading to the recommendation of a six-step process to BSS program implementation.

SECURITY IN PRACTICE

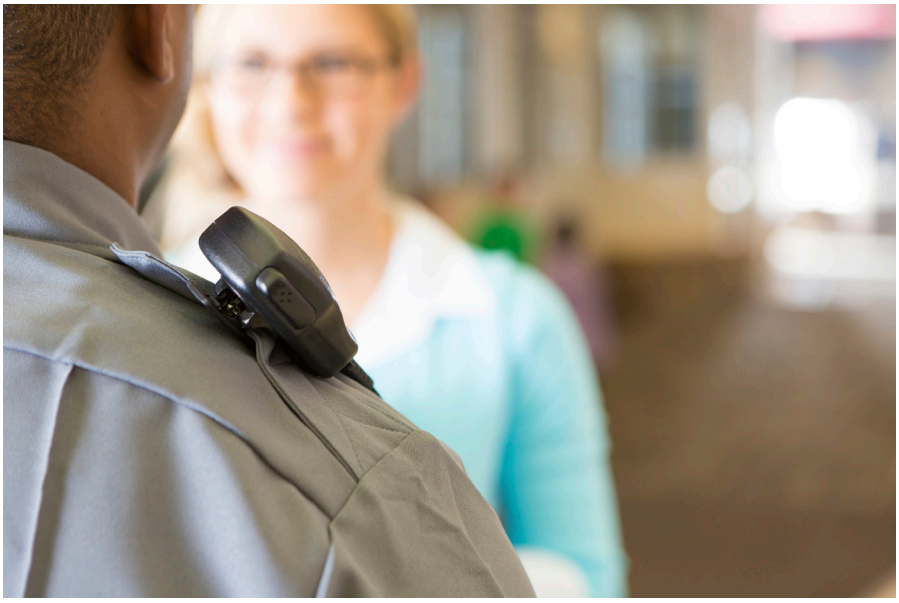
### SYSTEMATIC THREAT ASSESSMENT: HOW TO ADAPT SECURITY MEASURES BASED ON THE RESEARCH ON LATEST THREATS

To prevent acts of unlawful interference against civil aviation, knowledge about new threats is of fundamental importance when it comes to the adaption of security measures in an efficient and effective way. But which sources have to be tapped into and how must different emerging threats be weighted? CASRA developed and implemented a Systematic Threat Assessment (STA) to detect and prioritize latest threat scenarios and to develop appropriate defense strategies.

# APPROACHING SECURITY FROM ANOTHER ANGLE - BEHAVIORAL SECURITY SCREENING

Text: Sandrina Ritzmann

**Security screening processes at airports are still mainly focused on finding prohibited items. However, a growing number of authorities worldwide are interested in security measures at airports that also focus their attention on malicious intent: Trained personnel are scanning travelers for suspicious behavioral cues to identify wrongdoers. However, the question what form such a behavioral security screening (BSS) program should take or how it should be implemented is still in an investigation phase. CASRA conducted an 18-months scoping study, leading to the recommendation of a six-step process to BSS program implementation.**



Protecting civil aviation with suitable security measures is vital for society and economy. Aviation security screening is an essential component of these measures. The traditional approach in airport security screening is based on technology, airport security officers and processes to detect prohibited items on passengers and in their belongings. A more recent approach is based on detecting suspicious behavior of persons as an indicator of malicious intent. This approach is complementary to the traditional approach because it is not dependent on detection technology and has the potential to find also new and emerging threats which might not be detected as effectively otherwise.

The scoping study CASRA conducted in this area was funded by the Federal Office of Civil Aviation (FOCA) within its *Special Financing of Civil Aviation* fund. The goal of the study was to create a scientifically solid and practically relevant foundation for the discussion on how behavioral security screening could be implemented. A literature review combined with 13 expert interviews, a training pilot study and four round table discussions served to collect and analyze information on different aspects that are relevant to assess BSS and its implementation. To condense the large amount of data we collected, a process with the following six steps was proposed (see Fig. 1): Needs analysis, process definition, competence definition, selection and training, implementation and evaluation. The goal of this process is to pursue the implementation of BSS based on a scientifically well-founded approach. This article presents you with a summary of the six steps as an attempt to share the most important study results with our readers.

## NEEDS ANALYSIS

To suitably design and implement a BSS program, some groundwork is inevitable. Therefore, in the needs analysis phase, the objectives of a given security system should be examined to define how and to what extent BSS can support their achievement. Apart from security as an outcome, many other objectives might be relevant. An aspect that is often forgotten over the technical, economical and regulatory considerations and that is therefore highlighted here are the people who work in the security system. From the perspective of organizational psychology, it must be pointed out that the design of meaningful tasks for officers should be made a goal and a priority to increase job satisfaction, motivation, and performance ([1]). We will come back to this in the section on implementation.

After the examination of objectives, it should be determined which different options exist to implement BSS to be able to choose the most viable, effective and efficient one for a given situation. A number of different approaches were identified in our study. Their most important distinguishing factor is the importance that is ascribed to observation of behavior versus conversa-

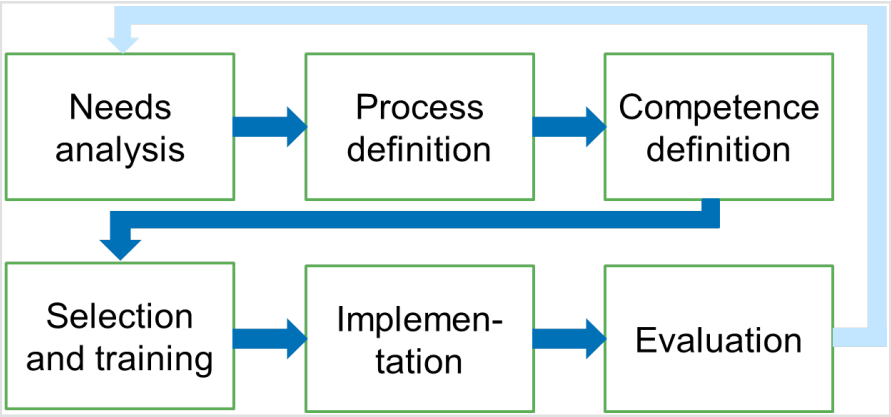



*Figure 1:* Six phases for implementing BSS

tion with a person. Observation is unobtrusive and goes mostly unnoticed by travelers, passers-by or staff while conversations and strategic questions can help to trigger behavioral cues to malicious intent that would not have been shown otherwise.

Aside from choosing the suitable approach to BSS, other decisions need to be taken, for example the specific location where to implement it (check-in, security checkpoint, public spaces etc.), or the way the BSS task should be designed (e.g. additional task for existing officers or separate task with dedicated officers). These decisions lead to the next phase, the process definition.

## PROCESS DEFINITION

In the needs analysis phase, a framework was developed consisting of the objectives and the desired scope of a BSS program. In the process definition phase, the framework should be "filled" with the concrete design of the BSS process. As a result of the CASRA scoping study, a specific BSS scenario with a defined process was proposed based on the outcomes of four round table discussions with relevant stakeholders (airports, security service providers, police, and handling agents). The analysis of the discussions led to an example scenario that allocates the responsibility for the implementation of BSS to the airports, with the regulating agency responsible for the definition and inspection of requirements. The example scenario focuses on BSS at the security checkpoint, but it can be combined with additional BSS measures in other areas of the aviation system. Against the background of our scoping study, the limited scope of the example scenario was chosen to enable a possible future trial in a scientific field study that demands a controlled setting. The scenario assumes that, based on an assessment of the necessary skills and abilities, existing staff is trained in BSS. The main concept of the example scenario is that passengers are observed and/or casually questioned within the regular process at the checkpoint. Ideally, different BSS "touch points" are put in place. The separate touch points can be combined or operated independently, depending on the security needs. A set-up with different touch points along with the security process also fosters unpredictability.

Further research should evaluate viable BSS scenarios such as the one proposed in the CASRA scoping study and investigate their effects on security and facilitation in controlled trials accompanied by scientific field studies. The topic of evaluation will be taken up again later in this article.

## COMPETENCE DEFINITION

The next phase in program implementation is the definition of the necessary competences that BSS officers need to successfully identify persons with negative intent. These competences depend on the approach chosen in the process definition phase. In an observation approach to BSS, other competences are relevant than in an approach where conversation plays a more central role.

The CASRA scoping study yielded some inputs from the expert interviews on the competences of BSS officers. It was suggested that a level of intelligence is required that allows officers to combine information and interpret observations in a larger context. Cognitive skills such as high memory performance or face and pattern recognition were deemed important. Communication, interviewing and interpersonal skills are listed as necessary when the BSS approach involves conversations with the passengers. The ability to attentively observe people over a longer period of time and BSS officers' capability of critically reflecting their own presuppositions and preconceptions were named as well. These expert inputs provide some ideas on important competences. However, in a BSS trial accompanied by a field study, competences should be scientifically defined and measured along with job performance data of the BSS officers. Statistical analyses could then show which criteria have the strongest links to performance and lead to further insights on the most relevant aspects. The next phase after the definition of the necessary competences is to explore and decide which of these competences can

be trained and which need to be covered already in the selection process.

## SELECTION & TRAINING

In this phase, the selection and training processes for the BSS program need to be defined. Traditionally, selection and aptitude testing covers cognitive abilities, personality traits or prerequisite behavior and skills. Training, on the other hand, targets knowledge that can be acquired, and specific behavioral aspects of job performance ([2]). This rough classification, ideally in combination with expert opinions, can serve as a starting point to determine which competences are prerequisites for the job and relevant for selection and which competences can be acquired through training. Based on this, the first draft of a selection test battery can be designed, along with a training course. In a next step, a field study where officers are selected and trained should serve to determine which abilities or traits predict job performance best even if the person has never done the job before (so-called predictive validity). Based on this, the definite selection test battery for the program at hand can be defined. Ideally, not only the selection test battery is evaluated and refined in a field study, but also the BSS training course. Our scoping study on BSS included a training pilot study that led to first positive results. Two training courses differing in content and didactic concept could be evaluated. Despite large differences in the design of the two types of training, participants in both courses showed favorable reactions and reported a gain of knowledge and positive attitudes towards BSS training. Also, both training designs were favorably rated by the participants. Further research in this area, ideally including behavioral performance tests after training, is highly recommended.[1]

## IMPLEMENTATION

From the viewpoint of work and organizational psychology, one key aspect with regard to program implementation will be highlighted here, although other aspects such as change management or sound project planning are important as well: the implementation of work design measures that foster job satisfaction, performance and motivation. These measures should already be planned during the needs analysis and process definition phases. However, in the implementation phase, special emphasis is necessary to assure that they do not stay merely cosmetic arrangements. Researchers have defined five important job characteristics - skill variety, task identity, task significance, autonomy and feedback ([1]). If the position or job of a BSS officer is defined and implemented accordingly, high performance as well as high satisfaction and motivation can be expected. It should contain a set of different tasks demanding various skills, e.g. manual bag search, communication with passengers and also BSS. This is skill variety. A high task identity, which signifies the execution of a whole task, can for example be achieved if security officers who perform hand searches of baggage or pat-downs of passengers can have a BSS-focused conversation with the passenger if they wish to acquire more information on a traveler. In order to underline the task significance and hence importance of the security screener job, it is advisable to regularly inform the employees on relevant security issues, averted attacks and success rates. Autonomy is fostered if a certain leeway in decision-making how to proceed with a passenger is granted to the BSS officers. Feedback should be given based on regular performance appraisals by supervisors, covert tests, passenger throughput, passenger satisfaction etc. Such data is available if a sound evaluation process is put in place, which leads us to the last one of the six steps.

## EVALUATION

A central aspect of any scientific field study or implementation of a full BSS program is the evaluation of program effectiveness and efficiency. This step serves to generate vital information that should be fed back to the needs analysis to determine whether any parameters need to be changed to achieve continuous improvement. In the evaluation phase, it needs to be defined what should actually be measured - the performance indicators (PIs) - and how to measure them. The central PI is certainly the detection performance of a BSS system. It is advisable to include the detection of different types of malicious acts (terrorist activities, drug trafficking, contraband trade etc.) and also covert tests in the measurement of detection performance. Other measures such as Threat Image Projection (TIP) performance could also be used to monitor the relationship of the detection of malicious intent and the detection of prohibited items, if this seems feasible. Important PIs covering the facilitation aspect of the security system are screening time and passenger satisfaction. The last group of PIs that is relevant is related to work design and consists of the measurement of the described job characteristics (see "implementation") and the assumed positive outcomes (e.g. job satisfaction; [1]). Standardized instruments exist that measure task design or subjective outcomes of work (e.g. [5]). It is highly advisable to evaluate this group of PIs to gauge the effect of BSS on job satisfaction, performance or motivation, in order to avoid negative outcomes of this new complementary or additional task.

[1] Readers familiar with training evaluation might recognize Kirkpatrick's hierarchical model of training outcomes ([3]). In our training pilot study, we focused on the first two levels (reactions, learning and attitudes). Behavior and organizational results (level 3 and 4) were not included.

Summing up the CASRA scoping study, we conclude that BSS is a security screening approach with the potential to find malicious intent and emerging threats which might not be detected as effectively otherwise. The careful creation of the BSS task also offers the opportunity to rethink job and task design so that the work of staff involved in security processes is motivating and satisfying. The study led to a number of highly relevant insights and the definition of the six-step process shown above. Designing, implementing and evaluating BSS according to this process can offer scientifically well-founded conclusions on program effectiveness and efficiency. Future applied research projects in this area should foster the close collaboration of practitioners, regulators and researchers to implement pilot programs, generate results on how BSS is best designed and implemented and harvest the fruits of science and practice going hand in hand to further advance aviation security.

## REFERENCES

[1] Hackman, J. R. & Oldham, G. R. (1976). Motivation through the design of work: Test of a theory. *Organizational Behavior and Human Performance, 16,* 250-279.

[2] Schuler, H. (2001). *Lehrbuch der Personalpsychologie [textbook on personnel psychology].* Göttingen: Hogrefe.

[3] Kirkpatrick, D. L. (1998). *Evaluating training programs: The four levels (2nd edition).* San Francisco: Berrett-Koehler Publishers.

[4] Muchinsky, P. M. (2012). *Psychology applied to work.* Summerfield, NC: Hypergraphic Press.

[5] Hackman, J. R. & Oldham, G. R. (1975). Development of job diagnostic survey. *Journal of Applied Psychology, 60,* 159-170.

# SYSTEMATIC THREAT ASSESSMENT: HOW TO ADAPT SECURITY MEASURES BASED ON THE RESEARCH ON LATEST THREATS

Text: Florian Schmid

**To prevent acts of unlawful interference against civil aviation, knowledge about new threats is of fundamental importance when it comes to the adaption of security measures in an efficient and effective way. But which sources have to be tapped into and how must different emerging threats be weighted? CASRA developed and implemented a Systematic Threat Assessment to detect and prioritize latest threat scenarios and to develop appropriate defense strategies.**

The Systematic Threat Assessment (STA) is an essential part of a long-term CASRA research project which is funded by the Swiss Federal Office of Civil Aviation (FOCA). The main project goal is to increase the threat detection performance at airports by combining up-to-date intelligence with competence of security officers based on very regular changes to current training programs and unpredictable adaptations of the screening level. The definition or adaptation of training measures for security officers should ideally be based on information on recent incidents as well as new and emerging threats to stay in tune with current and future threat scenarios. Therefore, an intelligence-based approach for the definition of different training measures, and potentially also other countermeasures, was established. In a two-step procedure, information is first collected from different sources and then analyzed and assessed with regard to a number of factors to determine the threat potential of a scenario.

## SCANNING OF DIFFERENT SOURCES

Within the scope of the STA process, different public and non-public internet channels are systematically scanned for information that might be relevant for aviation security. The choice of sources that are taken into account is of high importance for the quality and conclusiveness of the analysis. Therefore, the scanning process and the sources were defined with great care. Figure 1 gives an overview on the source categories of the CASRA STA.

An important part of the STA is to find and collect information on aviation specific security incidents. For this purpose, a large number of so-called web alerts was set up with different publicly available web content detection services. Such tools allow the subscription to keywords and keyword combinations like for example "IED + aircraft". Whenever the subscribed keyword combination appears on the internet, an automatic alert message is sent out by the web content detection service. In this manner, a large number of web alerts are constantly being generated and have to be evaluated by CASRA analysts. To this end, an intelligence analysis process was established in which the raw alert content is rated and categorized in order to separate relevant from irrelevant information. By means of search engines and meta search engines, a more detailed research on the relevant information is then performed in the Surface Web, the regular internet. This procedure is also applied for certain anonymity networks in the Deep Web (e.g. the Tor network; see infobox for more information). The Surface Web and Deep Web searches not only provide information about past incidents, they also reveal information related to the planning and preparation of attacks. In summary, this extensive internet analysis provides a valuable overview about key elements

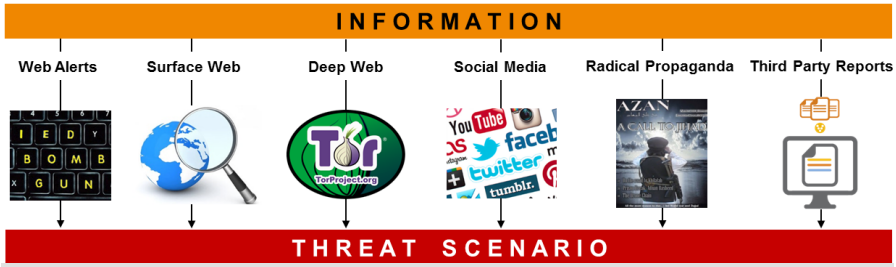



*Figure 1: Information sources*

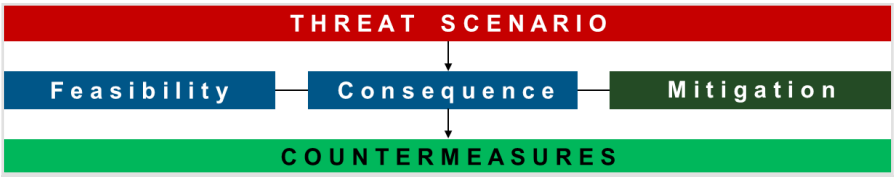



*Figure 2: Threat assessment process*

of threat scenarios such as the items and threat objects used, the availability of required items or previous successes with similar operation methods.

The fact that a large amount of relevant information also originates from online networking services or file sharing platforms shows the importance of paying particular attention to Social Media as well. This is why internet identities that are well known for regularly uploading and sharing relevant contents (e.g. manuals for the manufacturing of IEDs) are followed and monitored by the CASRA STA analysts in order to stay up-to-date about novel weapon types and attack techniques. In the same context, Radical Propaganda magazines represent another important source of information taken into account in the STA process. More than a dozen radical propaganda magazines that are available online in different languages are procured and scanned for relevant contents such as manuals, ideas or concrete calls to action.

As an addition to the large amount of information that is collected by the CASRA STA analysts themselves, threat reports from third-party suppliers in the field of web and technical intelligence services are included in the STA. This further supports the validity and conclusiveness of the sourcing of content.

## ASSESSMENT OF THREAT SCENARIOS

Information that is considered relevant is integrated into the STA database. However, due to the large amount of raw material, a process was defined that leads to a more conclusive list of potential threat scenarios. Subsequently, these scenarios are evaluated and assessed with regard to three specific factors:

- **Feasibility:** Is a threat scenario feasible, i.e. how easily are the necessary expertise and required materials available?
- **Consequence:** How high is the damage potential in terms of human, psychological and economic consequences?
- **Existing mitigation measures:** To what extent are damage minimizing measures already implemented?

In order to answer technical aspects of these questions, CASRA may rely on the expertise of supporting companies and competence centers at federal level. So far, this collaboration has resulted in a valuable network of experts whose assistance may be called upon if necessary. The knowledge that is gained within the framework of the particular evaluations is documented in threat reports that are sent to the relevant authorities who complement the information provided by CASRA with other information sources in considering the adaptation of existing and unpredictable measures.

Besides possible regulatory adaptations of security processes based on gained knowledge from the STA, countermeasures can also mean the

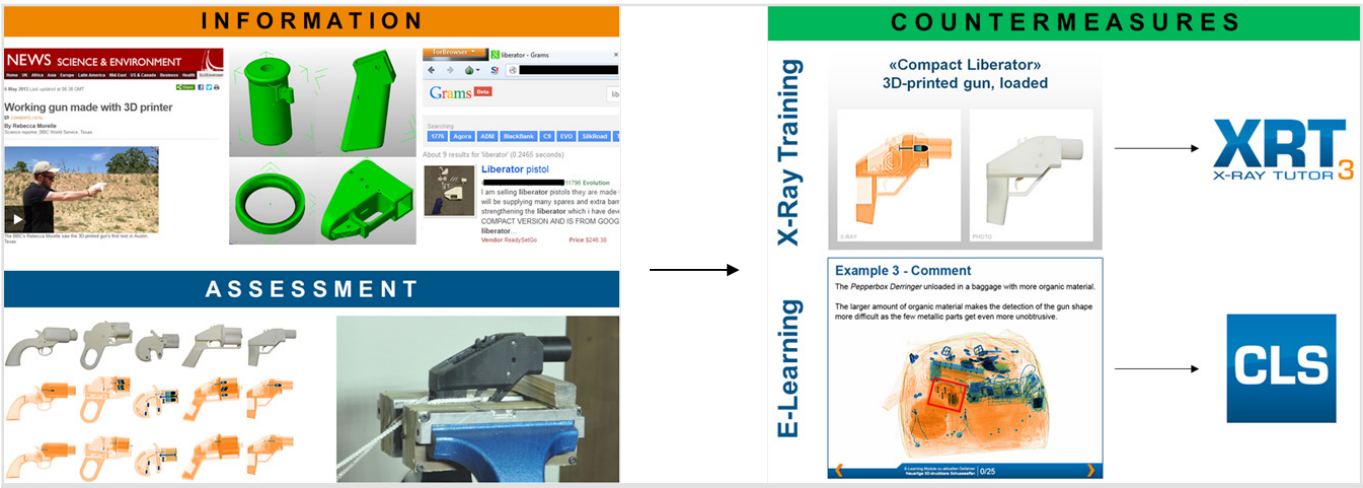



*Figure 3: 3D printed guns – from information to countermeasure*

implementation of new threat objects within the image libraries of the training program X-Ray Tutor 3 (XRT3) and/or the development of specific and up-to-date e-Learning modules for the CASRA Learning System (CLS).

## CASE STUDY: "3D PRINTED GUNS"

The example of 3D printed guns illustrates how the Systematic Threat Assessment operates from the first information up to the implementation of Fictional Threat Items (FTIs) of 3D printed guns in the X-ray training system XRT3 and the e-Learning platform CLS.

In May 2013, news channels reported the fabrication of the first working 3D printed gun called the Liberator. Comprehensive CASRA internet research showed that 3D files of different gun types could easily be downloaded on various file sharing platforms. In addition to that, a Deep Web evaluation of known marketplaces revealed the recent emergence of arms dealers who sell already printed 3D guns and deliver their products at a low price worldwide.

Within the framework of the STA and thanks to the collaboration with relevant Swiss authorities, CASRA was able to manufacture a number of different 3D guns in order to assess this novel threat scenario. In this manner, large-scale X-ray experiments with regard to their detectability, an evaluation of existing security measures as well as ballistic tests were conducted with the support of airports and federal competence centers. The results led to a report on this threat and the implementation of new FTIs showing different models of 3D printed guns into the training program XRT3. In addition to that, e-Learning modules for airport security personnel were developed and implemented in the CLS.

In summary, the STA supports CASRA in its efforts to produce highly relevant and up-to-date training material and it also serves as an additional source of information for relevant authorities in Switzerland. The main strengths of the STA are its structured process, its expert network and its timeliness. The constant evaluation of automatically generated news and the associated open source analysis allow the identification of novel threats in an early stage. This process facilitates the prompt elaboration of countermeasures such as the development of adequate training methods in order to sensitize security staff on latest threats.

## INFOBOX: DEEP WEB, TOR NETWORK

The expression "Deep Web" (also known as Deepnet, Invisible Web or Hidden Web) stands for the part of the internet content which is not indexed and therefore not retrievable by standard search engines. The indexed part of the Web which is retrievable by standard search engines is known as the Surface Web. The Deep Web is estimated to be hundreds of times bigger than the Surface Web. As a part of the Deep Web, the Tor network, accessible only by the dedicated Tor browser, enables users to surf the internet and publish content anonymously. Therefore it is used by a wide variety of people for both legal and illegal purposes.

Science & Security – CASRA Newsletter
ISSN 1664-5715
Published three times a year



CASRA
Thurgauerstrasse 39
8050 Zurich, Switzerland

Phone +41 (0)43 336 01 01
Fax +41 (0)43 336 01 00
E-mail info@casra.ch
Web www.casra.ch